Der sekundäre Verarbeitungsstandort

a) befindet sich in geografischer Entfernung vom primären Verarbeitungsstandort, damit er ein eigenes Risikoprofil aufweist und nicht von dem Ereignis, das sich am primären Standort ereignet hat, betroffen ist;

b) kann die Kontinuität kritischer oder wichtiger, mit dem primären Standort identischer Funktionen gewährleisten oder ein Leistungsniveau bereitstellen, mit dem sichergestellt wird, dass das Finanzunternehmen seine kritischen Vorgänge im Rahmen der Wiederherstellungsziele durchführt;

c) ist für das Personal des Finanzunternehmens unmittelbar zugänglich, damit die Kontinuität kritischer oder wichtiger Funktionen gewährleistet werden kann, falls der primäre Verarbeitungsstandort nicht mehr zur Verfügung steht.

(6) Bei der Festlegung der Vorgaben für die Wiederherstellungszeit und die Wiederherstellungspunkte jeder Funktion berücksichtigen die Finanzunternehmen, ob es sich um eine kritische oder wichtige Funktion handelt, sowie die potenziellen Gesamtauswirkungen auf die Markteffizienz. Mit diesen Zeitvorgaben ist sichergestellt, dass die vereinbarte Dienstleistungsgüte in Extremszenarien erreicht werden.

(7) Bei der Wiederherstellung nach IKT-bezogenen Vorfällen führen Finanzunternehmen die erforderlichen Prüfungen durch, einschließlich jeglicher Mehrfachprüfungen und Abgleiche, um die größtmögliche Datenintegrität sicherzustellen. Diese Prüfungen werden auch bei der Rekonstruktion von Daten externer Interessenträger durchgeführt, um sicherzustellen, dass alle Daten systemübergreifend einheitlich sind.

Artikel 13

Lernprozesse und Weiterentwicklung

(1) Finanzunternehmen verfügen über Kapazitäten und Personal, um Informationen über Schwachstellen und Cyberbedrohungen, IKT-bezogene Vorfälle, insbesondere Cyberangriffe, zu sammeln und ihre wahrscheinlichen Auswirkungen auf ihre digitale operationale Resilienz zu untersuchen.

(2) Nach Störungen ihrer Haupttätigkeiten infolge schwerwiegender IKT-bezogener Vorfälle sehen Finanzunternehmen nachträgliche Prüfungen IKT-bezogener Vorfälle vor, die die Ursachen für Störungen untersuchen und die erforderlichen Verbesserungen an IKT-Vorgängen oder im Rahmen der in Artikel 11 genannten IKT-Geschäftsfortführungsleitlinie identifizieren.

Finanzunternehmen, die keine Kleinstunternehmen sind, teilen den zuständigen Behörden auf Verlangen die Änderungen mit, die nach der Prüfung IKT-bezogener Vorfälle gemäß Unterabsatz 1 vorgenommen wurden.

Bei den in Unterabsatz 1 genannten nachträglichen Prüfungen IKT-bezogener Vorfälle wird ermittelt, ob die festgelegten Verfahren befolgt und die ergriffenen Maßnahmen wirksam waren, unter anderem in Bezug auf:

a) die Schnelligkeit bei der Reaktion auf Sicherheitswarnungen und bei der Bestimmung der Auswirkungen von IKT-bezogenen Vorfällen und ihrer Schwere;

b) die Qualität und Schnelligkeit bei der Durchführung forensischer Analysen, sofern dies als zweckmäßig erachtet wird;

c) die Wirksamkeit der Eskalation von Vorfällen innerhalb des Finanzunternehmens;

d) die Wirksamkeit interner und externer Kommunikation.

(3) Erkenntnisse aus gemäß den Artikeln 26 und 27 durchgeführten Tests der digitalen operationalen Resilienz und aus realen IKT-bezogenen Vorfällen, insbesondere Cyberangriffen, werden neben Herausforderungen, die sich bei der Aktivierung von IKT- Geschäftsfortführungsplänen und IKT-Reaktions- und Wiederherstellungsplänen ergeben, zusammen mit einschlägigen Informationen, die mit Gegenparteien ausgetauscht und im Rahmen aufsichtlicher Überprüfungen bewertet werden, kontinuierlich ordnungsgemäß in den IKT-Risikobewertungsprozess einbezogen. Diese Erkenntnisse bilden die Grundlage für angemessene Überprüfungen relevanter Komponenten des IKT-Risikomanagementrahmens gemäß Artikel 6 Absatz 1.

(4) Finanzunternehmen überwachen die Wirksamkeit der Umsetzung ihrer Strategie für die digitale operationale Resilienz gemäß Artikel 6 Absatz 8. Dabei erfassen sie die Entwicklung der IKT-Risiken im Zeitverlauf, untersuchen Häufigkeit, Art, Ausmaß und Entwicklung IKT-bezogener Vorfälle, insbesondere Cyberangriffe und deren Muster, um das Ausmaß der IKT-Risiken — insbesondere in Bezug auf kritische oder wichtige Funktionen — zu verstehen und die Cyberreife und die Abwehrbereitschaft des Finanzunternehmens zu verbessern.

(5) Leitende IKT-Mitarbeiter erstatten dem Leitungsorgan mindestens einmal jährlich über die in Absatz 3 genannten Feststellungen Bericht und geben Empfehlungen ab.

(6) Finanzunternehmen entwickeln Programme zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz, die im Rahmen ihrer Programme für die Mitarbeiterschulung obligatorisch sind. Diese Programme und Schulungen gelten für alle Beschäftigten und die Geschäftsleitung und sind so komplex, dass sie deren jeweiligem Aufgabenbereich angemessen sind. Gegebenenfalls nehmen die Finanzunternehmen entsprechend Artikel 30 Absatz 2 Buchstabe i auch IKT-Drittdienstleister in ihre einschlägigen Schulungsprogramme auf.

(7) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, überwachen einschlägige technologische Entwicklungen fortlaufend — auch um die möglichen Auswirkungen des Einsatzes solcher neuen Technologien auf die Anforderungen an die IKT-Sicherheit und die digitale operationale Resilienz zu verstehen. Sie halten sich über die neuesten Prozesse für das IKT-Risikomanagement auf dem Laufenden, um gegenwärtige oder neue Formen von Cyberangriffen wirksam abzuwehren.

Artikel 14

Kommunikation

(1) Als Teil des IKT-Risikomanagementrahmens gemäß Artikel 6 Absatz 1 verfügen Finanzunternehmen über Kommunikationspläne, die je nach Sachlage eine verantwortungsbewusste Offenlegung zumindest von schwerwiegenden IKT-bezogenen Vorfällen oder Schwachstellen gegenüber Kunden und anderen Finanzunternehmen sowie der Öffentlichkeit ermöglichen.

(2) Als Teil des IKT-Risikomanagementrahmens setzen Finanzunternehmen Kommunikationsstrategien für interne Mitarbeiter und externe Interessenträger um. Bei Kommunikationsleitlinien für Mitarbeiter wird berücksichtigt, dass zwischen dem Personal, das am IKT-Risikomanagement, insbesondere im Bereich Reaktion und Wiederherstellung, beteiligt ist, und dem zu informierendem Personal unterschieden werden muss.

(3) Mindestens eine Person im Finanzunternehmen ist mit der Umsetzung der Kommunikationsstrategie für IKT-bezogene Vorfälle beauftragt und nimmt zu diesem Zweck die entsprechende Aufgabe gegenüber der Öffentlichkeit und den Medien wahr.

Artikel 15

Weitere Harmonisierung von Tools, Methoden, Prozessen und Richtlinien für IKT-Risikomanagement

Die ESA entwickeln über den Gemeinsamen Ausschuss in Abstimmung mit der Agentur der Europäischen Union für Cybersicherheit (ENISA) gemeinsame Entwürfe technischer Regulierungsstandards für folgende Zwecke:

a) die Festlegung weiterer Elemente, die in die in Artikel 9 Absatz 2 genannten Richtlinien, Verfahren, Protokolle und Tools für IKT-Sicherheit aufzunehmen sind, um die Sicherheit von Netzwerken zu gewährleisten, angemessene Schutzvorrichtungen gegen Eindringen und Missbrauch von Daten zu ermöglichen, die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten, einschließlich kryptografischer Techniken, zu wahren und eine präzise und rasche Datenübermittlung ohne wesentliche Störungen und unangemessene Verzögerungen zu gewährleisten;

b) die Entwicklung weiterer Komponenten der Kontrollen von Zugangs- und Zugriffsrechten gemäß Artikel 9 Absatz 4 Buchstabe c und der damit verbundenen Personalpolitik, mit denen Zugangsrechte, Verfahren für Erteilung und Widerruf von Rechten, die Überwachung anomalen Verhaltens in Bezug auf IKT-Risiken durch angemessene Indikatoren — auch für Netzwerknutzungsmuster, Zeiten, IT-Aktivität und unbekannte Geräte — spezifiziert werden;

c) die Weiterentwicklung der in Artikel 10 Absatz 1 genannten Mechanismen, die eine umgehende Erkennung anomaler Aktivitäten ermöglichen, sowie der in Artikel 10 Absatz 2 genannten Kriterien, die Verfahren für die Erkennung IKT-bezogener Vorfälle und die damit verbundenen Reaktionsprozesse auslösen;

d) die Spezifizierung der in Artikel 11 Absatz 1 genannten Komponenten der IKT-Geschäftsfortführungsleitlinie;

e) die Spezifizierung der Tests von IKT-Geschäftsfortführungsplänen gemäß Artikel 11 Absatz 6, damit bei diesen Tests Szenarien, in denen die Qualität der Bereitstellung einer kritischen oder wichtigen Funktion auf ein inakzeptables Niveau absinkt oder diese Funktion ganz ausfällt, und die potenziellen Auswirkungen der Insolvenz oder sonstiger Ausfälle einschlägiger IKT-Drittdienstleister sowie gegebenenfalls die etwaigen politischen Risiken in den Rechtsordnungen in den Ländern und Gebieten der jeweiligen Anbieter gebührend berücksichtigt werden;

f) die Spezifizierung der Komponenten der in Artikel 11 Absatz 3 genannten IKT-Reaktions- und Wiederherstellungspläne;

g) die Spezifizierung von Inhalt und Form des in Artikel 6 Absatz 5 genannten Berichts über die Überprüfung des IKT-Risikomanagementrahmens.

Bei der Entwicklung dieser Entwürfe technischer Regulierungsstandards berücksichtigen die ESA die Größe und das Gesamtrisikoprofil des Finanzunternehmens sowie die Art, den Umfang und die Komplexität seiner Dienstleistungen, Tätigkeiten und Geschäfte, wobei sie etwaigen Besonderheiten, die sich aus der unterschiedlichen Art der Tätigkeiten in verschiedenen Finanzdienstleistungssektoren ergeben, gebührend Rechnung tragen.

Die ESA übermitteln der Kommission diese Entwürfe technischer Regulierungsstandards bis zum 17. Januar 2024.

Der Kommission wird die Befugnis übertragen, die vorliegende Verordnung durch Annahme der in Absatz 1 genannten technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

Artikel 16

Vereinfachter IKT-Risikomanagementrahmen

(1) Artikel 5 bis 15 gelten nicht für kleine und nicht verflochtene Wertpapierfirmen, entsprechend der Richtlinie (EU) 2015/2366 ausgenommene Zahlungsinstitute, entsprechend der Richtlinie 2013/36/EU ausgenommene Institute, für die die Mitgliedstaaten beschlossen haben, nicht von der in Artikel 2 Absatz 4 der vorliegenden Verordnung genannten Möglichkeit Gebrauch zu machen, nach der Richtlinie 2009/110/EG ausgenommene E-Geld-Institute und kleine Einrichtungen der betrieblichen Altersversorgung.

Unbeschadet des Unterabsatzes 1 müssen die in Unterabsatz 1 genannten Stellen

a) einen soliden und dokumentierten IKT-Risikomanagementrahmen errichten und aufrechterhalten, in dem die Mechanismen und Maßnahmen für ein rasches, effizientes und umfassendes Management des IKT-Risikos, einschließlich des Schutzes der einschlägigen physischen Komponenten und Infrastrukturen, detailliert sind;

b) die Sicherheit und das Funktionieren aller IKT-Systeme fortlaufend überwachen;

c) die Auswirkungen von IKT-Risiken minimieren, indem solide, resiliente und aktualisierte IKT-Systeme, -Protokolle und -Tools, die zur Unterstützung der Durchführung ihrer Tätigkeiten und zur Bereitstellung von Diensten angemessen sind, verwendet werden, und in angemessener Weise die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten in den Netzwerk- und Informationssystemen schützen;

d) eine rasche Ermittlung und Aufdeckung der Ursachen von IKT-Risiken und -Anomalien in den Netzwerk- und Informationssystemen sowie eine rasche Handhabung von IKT-Vorfällen ermöglichen;

e) die wesentlichen Abhängigkeiten von IKT-Drittdienstleistern ermitteln;

f) die Kontinuität kritischer oder wichtiger Funktionen durch Geschäftsfortführungspläne sowie Gegen- und Wiederherstellungsmaßnahmen, die zumindest Sicherungs- und Wiedergewinnungsmaßnahmen umfassen, gewährleisten;

g) die unter Buchstabe f genannten Pläne und Maßnahmen sowie die Wirksamkeit der gemäß den Buchstaben a und c durchgeführten Kontrollen regelmäßig testen;

h) gegebenenfalls die relevanten operativen Schlussfolgerungen, die sich aus den Tests gemäß Buchstabe g und der Analyse nach einem Vorfall ergeben, in den IKT-Risikobewertungsprozess einbeziehen und entsprechend dem Bedarf und dem IKT-Risikoprofil Programme zur Sensibilisierung für IKT-Sicherheit sowie Schulungen zur digitalen operationalen Resilienz für Personal und Management entwickeln.

(2) Der in Absatz 1 Unterabsatz 2 Buchstabe a genannte IKT-Risikomanagementrahmen wird regelmäßig und bei Auftreten schwerwiegender IKT-bezogener Vorfälle entsprechend den aufsichtsrechtlichen Anweisungen dokumentiert und überprüft. Der Rahmen wird auf der Grundlage der bei Umsetzung und Überwachung gewonnenen Erkenntnisse kontinuierlich verbessert. Der zuständigen Behörde wird auf Anfrage ein Bericht über die Überprüfung des IKT-Risikomanagementrahmens vorgelegt.

(3) Die ESA entwickeln über den Gemeinsamen Ausschuss in Abstimmung mit der ENISA gemeinsame Entwürfe technischer Regulierungsstandards für die folgenden Zwecke:

a) Spezifizierung der Elemente, die in den in Absatz 1 Unterabsatz 1 Buchstabe a genannten IKT-Risikomanagementrahmen aufzunehmen sind;

b) Spezifizierung der Elemente in Bezug auf Systeme, Protokolle und Tools zur Minimierung der in Absatz 1 Unterabsatz 2 Buchstabe c genannten Auswirkungen von IKT-Risiken, um die Sicherheit der Netzwerke zu gewährleisten, angemessene Schutzvorkehrungen gegen Eindringen und Datenmissbrauch zu ermöglichen und die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten zu wahren;

c) Spezifizierung der Komponenten der in Absatz 1 Unterabsatz 2 Buchstabe f genannten IKT-Geschäftsfortführungspläne;

d) Spezifizierung der Vorschriften über die Tests der Geschäftsfortführungspläne und Gewährleistung der Wirksamkeit der Kontrollen gemäß Absatz 1 Unterabsatz 2 Buchstabe g und Gewährleistung, dass bei diesen Tests Szenarien, in denen die Qualität der Bereitstellung einer kritischen oder wichtigen Funktion auf ein inakzeptables Niveau absinkt oder diese Funktion ganz ausfällt, gebührend berücksichtigt werden;

e) nähere Spezifizierung von Inhalt und Form des in Absatz 2 genannten Berichts über die Überprüfung des IKT-Risikomanagementrahmens.

Bei der Entwicklung dieser Entwürfe technischer Regulierungsstandards berücksichtigen die ESA die Größe und das Gesamtrisikoprofil des Finanzunternehmens sowie die Art, den Umfang und die Komplexität seiner Dienstleistungen, Tätigkeiten und Geschäfte.

Die ESA übermitteln der Kommission die Entwürfe dieser technischen Regulierungsstandards bis zum 17. Januar 2024.

Der Kommission wird die Befugnis übertragen, die vorliegende Verordnung durch Annahme der in Unterabsatz 1 genannten technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

KAPITEL III

Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle

Artikel 17

Prozess für die Behandlung IKT-bezogener Vorfälle

(1) Finanzunternehmen bestimmen einen Prozess für die Behandlung IKT-bezogener Vorfälle, richten diese ein und wenden sie an, um IKT-bezogene Vorfälle zu erkennen, zu behandeln und zu melden.

(2) Finanzunternehmen erfassen alle IKT-bezogenen Vorfälle und erheblichen Cyberbedrohungen. Finanzunternehmen richten angemessene Verfahren und Prozesse ein, um die kohärente und integrierte Überwachung, Handhabung und Weiterverfolgung IKT-bezogener Vorfälle zu gewährleisten, um sicherzustellen, dass Ursachen ermittelt, dokumentiert und angegangen werden, um das Auftreten solcher Vorfälle zu verhindern.

(3) Durch den in Absatz 1 genannten Prozess für die Behandlung IKT-bezogener Vorfälle

a) werden Frühwarnindikatoren eingesetzt;

b) werden Verfahren zur Ermittlung, Nachverfolgung, Protokollierung, Kategorisierung und Klassifizierung IKT-bezogener Vorfälle entsprechend ihrer Priorität und Schwere und entsprechend der Kritikalität der betroffenen Dienste entsprechend den in Artikel 18 Absatz 1 genannten Kriterien eingerichtet;

c) werden Funktionen und Zuständigkeiten zugewiesen, die bei verschiedenen Arten von IKT-bezogenen Vorfällen und -Szenarien aktiviert werden müssen;

d) werden gemäß Artikel 14 Pläne für die Kommunikation mit Personal, externen Interessenträgern und Medien sowie für die Benachrichtigung von Kunden, für interne Eskalationsverfahren, einschließlich IKT-bezogener Kundenbeschwerden, und für die Bereitstellung von Informationen an andere Finanzunternehmen, die als Gegenparteien fungieren, ausgearbeitet, je nach Sachlage;

e) wird sichergestellt, dass zumindest schwerwiegende IKT-bezogene Vorfälle der zuständigen höheren Führungsebene gemeldet werden und die Geschäftsleitung informiert wird, wobei die Auswirkungen und Gegenmaßnahmen und zusätzliche Kontrollen erläutert werden, die infolge dieser IKT-bezogenen Vorfälle einzurichten sind;

f) werden Verfahren für Reaktionsmaßnahmen bei IKT-bezogenen Vorfällen eingerichtet, um Auswirkungen zu mindern und sicherzustellen, dass die Dienste zeitnah verfügbar und sicher werden.

Artikel 18

Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen

(1) Finanzunternehmen klassifizieren IKT-bezogene Vorfälle und bestimmen deren Auswirkungen anhand folgender Kriterien:

a) Anzahl und/oder Relevanz der Kunden oder anderer Gegenparteien im Finanzbereich, die von dem IKT-bezogenen Vorfall betroffen sind, und gegebenenfalls des Werts oder der Anzahl der davon betroffenen Transaktionen und ob der IKT-bezogene Vorfall einen Reputationsschaden verursacht hat;

b) Dauer des IKT-bezogenen Vorfalls, einschließlich der Ausfallzeiten des Dienstes;

c) geografische Ausbreitung der von dem IKT-bezogenen Vorfall betroffenen Gebiete, insbesondere wenn mehr als zwei Mitgliedstaaten betroffen sind;

d) die mit dem IKT-bezogenen Vorfall verbundenen Verfügbarkeits-, Authentizitäts-, Integritäts- oder Vertraulichkeitsverluste von Daten;

e) Kritikalität der betroffenen Dienste, einschließlich der Transaktionen und Geschäfte des Finanzunternehmens;

f) wirtschaftliche Auswirkungen — insbesondere direkte und indirekte Kosten und Verluste — des IKT-bezogenen Vorfalls auf absoluter und relativer Basis.

(2) Finanzunternehmen stufen Cyberbedrohungen auf der Grundlage der Kritikalität der risikobehafteten Dienste, einschließlich der Transaktionen und Geschäfte des Finanzunternehmens, der Anzahl und/oder Relevanz der betroffenen Kunden oder Gegenparteien im Finanzbereich und der geografischen Ausbreitung der Risikogebiete als erheblich ein.

(3) Die ESA erarbeiten über den Gemeinsamen Ausschuss in Abstimmung mit der EZB und der ENISA gemeinsame Entwürfe technischer Regulierungsstandards, in denen Folgendes präzisiert wird:

a) die in Absatz 1 genannten Kriterien, einschließlich der Wesentlichkeitsschwellen für die Bestimmung schwerwiegender IKT-bezogener Vorfälle oder gegebenenfalls schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfälle, die der Meldepflicht nach Artikel 19 Absatz 1 unterliegen;

b) die Kriterien, die von den zuständigen Behörden anzuwenden sind, um die Relevanz schwerwiegender IKT-bezogener Vorfälle oder gegebenenfalls schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfälle für die jeweils zuständigen Behörden in anderen Mitgliedstaaten zu bewerten, sowie die Einzelheiten in den Meldungen über schwerwiegende IKT-bezogene Vorfälle oder gegebenenfalls schwerwiegende zahlungsbezogene Betriebs- oder Sicherheitsvorfälle, die anderen zuständigen Behörden gemäß Artikel 19 Absätze 6 und 7 übermittelt werden müssen;

c) die in Absatz 2 genannten Kriterien, einschließlich hoher Wesentlichkeitsschwellen für die Bestimmung erheblicher Cyberbedrohungen.

(4) Bei der Ausarbeitung der in Absatz 3 genannten gemeinsamen Entwürfe technischer Regulierungsstandards berücksichtigen die ESA die in Artikel 4 Absatz 2 genannten Kriterien sowie von der ENISA entwickelte und veröffentlichte internationale Standards, Leitlinien und Spezifikationen, gegebenenfalls einschließlich Spezifikationen für andere Wirtschaftszweige. Für die Zwecke der Anwendung der in Artikel 4 Absatz 2 festgelegten Kriterien berücksichtigen die ESA gebührend, dass Kleinstunternehmen sowie kleine und mittlere Unternehmen ausreichende Ressourcen und Kapazitäten mobilisieren können müssen, um sicherzustellen, dass IKT-bezogene Vorfälle rasch bewältigt werden.

Die ESA übermitteln der Kommission diese allgemeinen Entwürfe technischer Regulierungsstandards bis zum 17. Januar 2024.

Der Kommission wird die Befugnis übertragen, diese Verordnung durch Annahme der in Absatz 3 genannten technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

Artikel 19

Meldung schwerwiegender IKT-bezogener Vorfälle und freiwillige Meldung erheblicher Cyberbedrohungen

(1) Finanzunternehmen melden der nach Artikel 46 jeweils zuständigen Behörde gemäß Absatz 4 schwerwiegende IKT-bezogene Vorfälle.

Unterliegt ein Finanzunternehmen der Aufsicht mehr als einer nach Artikel 46 zuständigen nationalen Behörde, so benennen die Mitgliedstaaten eine einzige zuständige Behörde als einschlägige zuständige Behörde, die für die Wahrnehmung der im vorliegenden Artikel aufgeführten Funktionen und Aufgaben verantwortlich ist.

Kreditinstitute, die gemäß Artikel 6 Absatz 4 der Verordnung (EU) Nr. 1024/2013 als bedeutend eingestuft wurden, melden schwerwiegende IKT-bezogene Vorfälle der gemäß Artikel 4 der Richtlinie 2013/36/EU benannten jeweils zuständigen nationalen Behörde, die diese Meldung unverzüglich an die EZB weiterleitet.

Für die Zwecke von Unterabsatz 1 erstellen Finanzunternehmen nach Erfassung und Analyse aller relevanten Informationen unter Verwendung der in Artikel 20 genannten Vorlage die Erstmeldung und die Meldungen nach Absatz 4 und übermitteln diese der zuständigen Behörde. Falls es aus technischen Gründen nicht möglich ist, die Erstmeldung unter Verwendung der Vorlage zu übermitteln, teilen die Finanzunternehmen dies der zuständigen Behörde auf anderem Wege mit.

Die Erstmeldung und die Meldungen nach Absatz 4 enthalten alle Informationen, die die zuständige Behörde benötigt, um die Signifikanz des schwerwiegenden IKT-bezogenen Vorfalls zu ermitteln und mögliche grenzüberschreitende Auswirkungen zu bewerten.

Unbeschadet der Meldung gemäß Unterabsatz 1 durch das Finanzunternehmen an die jeweils zuständige Behörde können die Mitgliedstaaten zusätzlich festlegen, dass einige oder alle Finanzunternehmen die Erstmeldung und jede Meldung nach Absatz 4 auch den gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden oder Computer-Notfallteams (computer security incident response teams — CSIRT) unter Verwendung der in Artikel 20 genannten Vorlage zur Verfügung stellen müssen.

(2) Finanzunternehmen können der jeweils zuständigen Behörde auf freiwilliger Basis erhebliche Cyberbedrohungen melden, wenn sie der Auffassung sind, dass die Bedrohung für das Finanzsystem, die Dienstnutzer oder die Kunden relevant ist. Die jeweils zuständige Behörde kann derartige Informationen anderen in Absatz 6 genannten einschlägigen Behörden zur Verfügung stellen.

Kreditinstitute, die gemäß Artikel 6 Absatz 4 der Verordnung (EU) Nr. 1024/2013 als bedeutend eingestuft wurden, können erhebliche Cyberbedrohungen auf freiwilliger Basis der gemäß Artikel 4 der Richtlinie 2013/36/EU benannten jeweils zuständigen nationalen Behörde melden, die diese Meldung unverzüglich an die EZB weiterleitet.

Die Mitgliedstaaten können festlegen, dass die Finanzunternehmen, die auf freiwilliger Basis eine Meldung gemäß Unterabsatz 1 vornehmen, diese Meldung auch an die gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten CSIRT erstatten können.

(3) Wenn ein schwerwiegender IKT-bezogener Vorfall auftritt und Auswirkungen auf die finanziellen Interessen von Kunden hat, unterrichten die Finanzunternehmen, sobald sie hiervon Kenntnis erlangt haben, ihre Kunden unverzüglich über den schwerwiegenden IKT-bezogenen Vorfall und die Maßnahmen, die ergriffen wurden, um die nachteiligen Auswirkungen eines solchen Vorfalls zu mindern.

Im Falle einer erheblichen Cyberbedrohung unterrichten die Finanzunternehmen gegebenenfalls ihre potenziell betroffenen Kunden über angemessene Schutzmaßnahmen, die diese ergreifen könnten.

(4) Finanzunternehmen legen innerhalb der in Artikel 20 Absatz 1 Buchstabe a Ziffer ii festzulegenden Fristen der jeweils zuständigen Behörde Folgendes vor:

a) eine Erstmeldung;

b) nach der Erstmeldung gemäß Buchstabe a eine Zwischenmeldung, sobald sich der Status des ursprünglichen Vorfalls erheblich geändert hat oder sich die Handhabung des schwerwiegenden IKT-bezogenen Vorfalls auf der Grundlage neuer verfügbarer Informationen geändert hat, gegebenenfalls gefolgt von aktualisierten Meldungen, wann immer eine entsprechende Statusaktualisierung vorliegt, sowie auf ausdrücklichen Antrag der zuständigen Behörde;

c) eine Abschlussmeldung, wenn die Ursachenanalyse abgeschlossen ist — unabhängig davon, ob bereits Minderungsmaßnahmen getroffen wurden oder nicht — und sich die tatsächlichen Auswirkungen beziffern lassen und Schätzungen ersetzen.

(5) Finanzunternehmen dürfen im Einklang mit den sektorspezifischen Rechtsvorschriften der Union und der Mitgliedstaaten die Meldepflichten nach diesem Artikel an einen Drittdienstleister auslagern. Bei einer solchen Auslagerung bleibt das Finanzunternehmen in vollem Umfang für die Erfüllung der Anforderungen für die Meldung von Vorfällen verantwortlich.

(6) Nach Eingang der Erstmeldung und jeder Meldung nach Absatz 4 übermittelt die zuständige Behörde auf der Grundlage der je nach Sachlage bestehenden jeweiligen Zuständigkeiten zeitnah Einzelheiten zu dem schwerwiegenden IKT-bezogenen Vorfall an die folgenden Empfänger:

a) die EBA, die ESMA oder die EIOPA;

b) die EZB, sofern es sich um Finanzunternehmen im Sinne von Artikel 2 Absatz 1 Buchstaben a, b und d handelt;

c) die zuständigen Behörden, die zentrale Anlaufstelle oder die CSIRT, die jeweils gemäß der Richtlinie (EU) 2022/2555 benannt oder eingerichtet werden;

d) die in Artikel 3 der Richtlinie 2014/59/EU genannten Abwicklungsbehörden und den Einheitlichen Abwicklungsausschuss (Single Resolution Board — SRB) in Bezug auf die in Artikel 7 Absatz 2 der Verordnung (EU) Nr. 806/2014 des Europäischen Parlaments und des Rates ([37]) genannten Unternehmen sowie in Bezug auf die in Artikel 7 Absatz 4 Buchstabe b und Absatz 5 der Verordnung (EU) Nr. 806/2014 genannten Unternehmen und Gruppen, wenn diese Einzelheiten Vorfälle betreffen, die ein Risiko für die Sicherstellung kritischer Funktionen im Sinne von Artikel 2 Absatz 1 Nummer 35 der Richtlinie 2014/59/EU darstellen; und

e) andere einschlägige Behörden nach nationalem Recht.

(7) Nach Erhalt der Informationen gemäß Absatz 6 bewerten die EBA, die ESMA oder die EIOPA und die EZB in Abstimmung mit der ENISA und in Zusammenarbeit mit der jeweils zuständigen Behörde, ob der schwerwiegende IKT-bezogene Vorfall für die zuständigen Behörden in anderen Mitgliedstaaten von Belang ist. Im Anschluss an diese Bewertung benachrichtigen die EBA, die ESMA oder die EIOPA die jeweils zuständigen Behörden in anderen Mitgliedstaaten entsprechend. Die EZB unterrichtet die Mitglieder des Europäischen Systems der Zentralbanken über die für das Zahlungssystem relevanten Aspekte. Auf der Grundlage dieser Unterrichtung treffen die zuständigen Behörden gegebenenfalls alle für die unmittelbare Stabilität des Finanzsystems notwendigen Schutzvorkehrungen.

([37]) Verordnung (EU) Nr. 806/2014 des Europäischen Parlaments und des Rates vom 15. Juli 2014 zur Festlegung einheitlicher Vorschriften und eines einheitlichen Verfahrens für die Abwicklung von Kreditinstituten und bestimmten Wertpapierfirmen im Rahmen eines einheitlichen Abwicklungsmechanismus und eines einheitlichen Abwicklungsfonds sowie zur Änderung der Verordnung (EU) Nr. 1093/2010 (ABl. L 225 vom 30.7.2014, S. 1).

(8) Die von der ESMA gemäß Absatz 7 vorzunehmende Meldung berührt nicht die Verantwortung der zuständigen Behörde, die Einzelheiten des schwerwiegenden IKT-bezogenen Vorfalls umgehend an die einschlägige Behörde des Aufnahmemitgliedstaats weiterzuleiten, wenn ein Zentralverwahrer eine umfassende grenzüberschreitende Tätigkeit in dem Aufnahmemitgliedstaat ausübt, der schwerwiegende IKT-bezogene Vorfall wahrscheinlich schwerwiegende Folgen für die Finanzmärkte des Aufnahmemitgliedstaats hat und zwischen den zuständigen Behörden Kooperationsvereinbarungen in Bezug auf die Beaufsichtigung von Finanzunternehmen bestehen.

Artikel 20

Harmonisierung von Inhalt und Vorlagen von Meldungen

Die ESA erarbeiten über den Gemeinsamen Ausschuss und in Abstimmung mit der ENISA und der EZB

a) gemeinsame Entwürfe technischer Regulierungsstandards, um

   i) den Inhalt von Meldungen über schwerwiegende IKT-bezogene Vorfälle festzulegen, damit den in Artikel 18 Absatz 1 aufgeführten Kriterien Rechnung getragen wird und weitere Elemente einbezogen werden, wie z. B. Einzelheiten zur Feststellung der Relevanz der Meldungen für andere Mitgliedstaaten und die Frage, ob es sich dabei um einen schwerwiegenden zahlungsbezogenen Betriebs- oder Sicherheitsvorfall handelt;

   ii) die Fristen für die Erstmeldung und jede Meldung nach Artikel 19 Absatz 4 festzulegen;

   iii) den Inhalt der Meldung erheblicher Cyberbedrohungen festzulegen.

   Bei der Ausarbeitung dieser Entwürfe technischer Regulierungsstandards berücksichtigen die ESA die Größe und das Gesamtrisikoprofil des Finanzunternehmens sowie die Art, den Umfang und die Komplexität seiner Dienstleistungen, Tätigkeiten und Geschäfte, um insbesondere sicherzustellen, dass den Besonderheiten der Finanzsektoren für die Zwecke des vorliegenden Absatzes Buchstabe a Ziffer ii gegebenenfalls durch unterschiedliche Fristen Rechnung getragen wird, unbeschadet der Beibehaltung eines kohärenten Ansatzes für die Meldung IKT-bezogener Vorfälle gemäß dieser Verordnung und gemäß der Richtlinie (EU) 2022/2555. Die ESA legen — sofern zutreffend — eine Begründung vor, wenn sie von den im Rahmen jener Richtlinie verfolgten Ansätzen abweichen;

b) gemeinsame Entwürfe technischer Durchführungsstandards zur Festlegung von Standardformularen, Vorlagen und Verfahren für Finanzunternehmen zur Meldung eines schwerwiegenden IKT-bezogenen Vorfalls oder einer erheblichen Cyberbedrohung.

Die ESA übermitteln der Kommission die in Absatz 1 Buchstabe a genannten gemeinsamen Entwürfe technischer Regulierungsstandards und die in Absatz 1 Buchstabe b genannten gemeinsamen Entwürfe technischer Durchführungsstandards bis zum 17. Juli 2024.

Der Kommission wird die Befugnis übertragen, diese Verordnung durch Annahme der in Absatz 1 Buchstabe a genannten gemeinsamen technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

Der Kommission wird die Befugnis übertragen, die in Absatz 1 Buchstabe b genannten gemeinsamen technischen Durchführungsstandards gemäß Artikel 15 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 (EU) Nr. 1095/2010 zu erlassen.

Artikel 21

Zentralisierung der Berichterstattung über schwerwiegende IKT-bezogene Vorfälle

(1) Die ESA erstellen über den Gemeinsamen Ausschuss und in Abstimmung mit der EZB und der ENISA einen gemeinsamen Bericht, in dem sie die Durchführbarkeit einer weiteren Zentralisierung der Meldung von Vorfällen durch die Einrichtung einer einheitlichen EU-Plattform für die Meldung schwerwiegender IKT-bezogener Vorfälle durch Finanzunternehmen bewerten. In dem gemeinsamen Bericht werden Möglichkeiten sondiert, um den Meldefluss zu IKT-bezogenen Vorfällen zu erleichtern, damit verbundene Kosten zu senken und thematische Analysen zur Erhöhung aufsichtlicher Konvergenz zu unterstützen.

(2) Der in Absatz 1 genannte gemeinsame Bericht umfasst mindestens die folgenden Aspekte:

a) Voraussetzungen für die Einrichtung einer einheitlichen EU-Plattform;

b) Vorteile, Grenzen und Risiken, einschließlich Risiken im Zusammenhang mit einer hohen Konzentration sensibler Informationen;

c) die erforderliche Fähigkeit zur Gewährleistung der Interoperabilität im Hinblick auf andere einschlägige Meldesysteme;

d) Elemente des Betriebsmanagements;

e) Voraussetzungen für die Mitgliedschaft;

f) technische Regelungen für den Zugang von Finanzunternehmen und zuständigen nationalen Behörden zur einheitlichen EU-Plattform;

g) eine vorläufige Bewertung der finanziellen Kosten, die durch die Einrichtung der operativen Plattform zur Unterstützung der einheitlichen EU-Plattform entstehen, einschließlich des erforderlichen Fachwissens.

(3) Die ESA übermitteln dem Europäischen Parlament, dem Rat und der Kommission den in Absatz 1 genannten Bericht bis zum 17. Januar 2025.

Artikel 22

Rückmeldungen von Aufsichtsbehörden

(1) Unbeschadet der technischen Informationen, Empfehlungen oder Abhilfe- und Folgemaßnahmen, die im Einklang mit dem nationalen Recht gegebenenfalls vom CSIRT gemäß Richtlinie (EU) 2022/2555 bereitgestellt werden können, bestätigt die zuständige Behörde nach Eingang der Erstmeldung und jeder Meldung nach Artikel 19 Absatz 4 den Eingang und kann, wenn möglich, dem Finanzunternehmen zeitnah sachdienliche und angemessene Rückmeldungen oder allgemein gehaltene Orientierungshilfen übermitteln, insbesondere durch Zurverfügungstellung relevanter anonymisierter Informationen und Erkenntnisse zu ähnlichen Bedrohungen, sowie auf Ebene des Unternehmens angewandte Abhilfemaßnahmen und Möglichkeiten zur Minimierung und Minderung nachteiliger Auswirkungen auf den gesamten Finanzsektor erörtern. Unbeschadet der aufsichtlichen Rückmeldung bleiben Finanzunternehmen in vollem Umfang für die Handhabung und die Folgen der gemäß Artikel 19 Absatz 1 gemeldeten IKT-bezogenen Vorfälle verantwortlich.

(2) Die ESA berichten jährlich über den Gemeinsamen Ausschuss in anonymisierter und aggregierter Form über schwerwiegende IKT-bezogene Vorfälle, deren Einzelheiten von den zuständigen Behörden gemäß Artikel 19 Absatz 6 übermittelt werden, und geben dabei mindestens die Zahl schwerwiegender IKT-bezogener Vorfälle, ihre Art und ihre Auswirkungen auf die Geschäftstätigkeit von Finanzunternehmen oder Kunden sowie die ergriffenen Abhilfemaßnahmen und die Kosten an.

Die ESA geben Warnungen heraus und erstellen allgemein gehaltene Statistiken, um die Bewertungen von Bedrohungen und Schwachstellen im IKT-Bereich zu unterstützen.

Artikel 23

Zahlungsbezogene Betriebs- oder Sicherheitsvorfälle, die Kreditinstitute, Zahlungsinstitute, Kontoinformationsdienstleister und E-Geld-Institute betreffen

Die Anforderungen in diesem Kapitel gelten auch für zahlungsbezogene Betriebs- oder Sicherheitsvorfälle, auch schwerwiegender Art, wenn sie Kreditinstitute, Zahlungsinstitute, Kontoinformationsdienstleister und E-Geld-Institute betreffen.

KAPITEL IV

Testen der digitalen operationalen Resilienz

Artikel 24

Allgemeine Anforderungen für das Testen der digitalen operationalen Resilienz

(1) Um die Vorbereitung auf die Handhabung IKT-bezogener Vorfälle zu bewerten, Schwächen, Mängel und Lücken in Bezug auf die digitale operationale Resilienz zu erkennen und Korrekturmaßnahmen umgehend umzusetzen, erstellen, pflegen und überprüfen Finanzunternehmen, die keine Kleinstunternehmen sind, unter Berücksichtigung der in Artikel 4 Absatz 2 aufgeführten Kriterien ein solides und umfassendes Programm für das Testen der digitalen operationalen Resilienz als integraler Bestandteil des in Artikel 6 genannten IKT-Risikomanagementrahmens.

(2) Das Programm für Tests der digitalen operationalen Resilienz umfasst eine Reihe von Bewertungen, Tests, Methoden, Verfahren und Tools, die gemäß den Artikeln 25 und 26 anzuwenden sind.

(3) Bei der Ausführung des in Absatz 1 genannten Programms für das Testen der digitalen operationalen Resilienz wenden Finanzunternehmen, die keine Kleinstunternehmen sind, unter Berücksichtigung der in Artikel 4 Absatz 2 aufgeführten Kriterien einen risikobasierten Ansatz an, wobei sie die sich entwickelnden IKT-Risikolandschaften, etwaige spezifische Risiken, denen das betreffende Finanzunternehmen ausgesetzt ist oder ausgesetzt sein könnte, die Kritikalität von Informationsassets und erbrachten Dienstleistungen sowie alle sonstigen Faktoren, die das Finanzunternehmen für angemessen hält, gebührend berücksichtigen.

(4) Finanzunternehmen, die keine Kleinstunternehmen sind, stellen sicher, dass Tests von unabhängigen, internen oder externen Parteien durchgeführt werden. Werden die Tests von einem internen Tester durchgeführt, stellen die Finanzunternehmen ausreichende Ressourcen bereit und tragen dafür Sorge, dass während der Konzeptions- und Durchführungsphase der Prüfung keine Interessenkonflikte entstehen.

(5) Finanzunternehmen, die keine Kleinstunternehmen sind, legen Verfahren und Leitlinien zur Priorisierung, Klassifizierung und Behebung aller während der Durchführung der Tests zutage getretenen Probleme fest und legen interne Validierungsmethoden fest, um sicherzustellen, dass alle ermittelten Schwächen, Mängel oder Lücken vollständig angegangen werden.

(6) Finanzunternehmen, die keine Kleinstunternehmen sind, stellen sicher, dass bei allen IKT-Systemen und -Anwendungen, die kritische oder wichtige Funktionen unterstützen, mindestens einmal jährlich angemessene Tests durchgeführt werden.

Artikel 25

Testen von IKT-Tools und -Systemen

(1) Das in Artikel 24 genannte Programm für die Tests der digitalen operationalen Resilienz beinhaltet im Einklang mit den in Artikel 4 Absatz 2 aufgeführten Kriterien die Durchführung angemessener Tests, wie etwa Schwachstellenbewertung und -scans, Open-Source-Analysen, Netzwerksicherheitsbewertungen, Lückenanalysen, Überprüfungen der physischen Sicherheit, Fragebögen und Scans von Softwarelösungen, Quellcodeprüfungen soweit durchführbar, szenariobasierte Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests und Penetrationstests.

(2) Zentralverwahrer und zentrale Gegenparteien führen Schwachstellenbewertungen durch, bevor Anwendungen und Infrastrukturkomponenten sowie IKT-Dienstleistungen, die kritische oder wichtige Funktionen des Finanzunternehmens unterstützen, eingesetzt oder wieder eingesetzt werden.

(3) Kleinstunternehmen führen die in Absatz 1 genannten Tests durch, indem sie einen risikobasierten Ansatz mit einer strategischen Planung für IKT-Tests kombinieren, wobei sie gebührend berücksichtigen, dass zwischen dem Umfang von Ressourcen und der Zeit, die für die IKT-Tests gemäß diesem Artikel aufzuwenden sind, einerseits, und der Dringlichkeit, der Art des Risikos, der Kritikalität von Informationsassets und erbrachten Dienstleistungen sowie allen sonstigen relevanten Faktoren, einschließlich der Fähigkeit des Finanzunternehmens, kalkulierte Risiken einzugehen, andererseits, ein ausgewogenes Verhältnis gewahrt werden muss.

Artikel 26

Erweiterte Tests von IKT-Tools, -Systemen und -Prozessen auf Basis von TLPT

(1) Gemäß Absatz 8 Unterabsatz 3 des vorliegenden Artikels ermittelte Finanzunternehmen, bei denen es sich weder um die in Artikel 16 Absatz 1 Unterabsatz 1 genannten Unternehmen noch um Kleinstunternehmen handelt, führen mindestens alle drei Jahre anhand von TLPT erweiterte Tests durch. Auf der Grundlage des Risikoprofils des Finanzunternehmens und unter Berücksichtigung der betrieblichen Gegebenheiten kann die zuständige Behörde das Finanzunternehmen erforderlichenfalls auffordern, die Häufigkeit dieser Tests zu verringern oder zu erhöhen.

(2) Jeder bedrohungsorientierte Penetrationstest schließt mehrere oder alle kritischen oder wichtigen Funktionen eines Finanzunternehmens ein und wird an Live-Produktionssystemen durchgeführt, die derartige Funktionen unterstützen.

Finanzunternehmen ermitteln alle relevanten zugrunde liegenden IKT-Systeme, -Prozesse und -Technologien, die kritische oder wichtige Funktionen und IKT-Dienstleistungen unterstützen, einschließlich derer, die diejenigen kritischen oder wichtigen Funktionen unterstützen, die an IKT-Drittdienstleister ausgelagert oder per Vertrag vergeben wurden.

Finanzunternehmen bewerten, welche kritischen oder wichtigen Funktionen ein TLPT einschließen muss. Der genaue Umfang von TLPT ist vom Ergebnis dieser Bewertung abhängig und wird von den zuständigen Behörden validiert.

(3) Sind IKT-Drittdienstleister in das Spektrum der TLPT einbezogen, ergreift das Finanzunternehmen alle erforderlichen Maßnahmen und Vorkehrungen, um die Einbindung dieser IKT-Drittdienstleister in die TLPT sicherzustellen, und trägt jederzeit die volle Verantwortung für die Gewährleistung der Einhaltung dieser Verordnung.

(4) Wenn vernünftigerweise davon auszugehen ist, dass sich die Einbindung eines IKT-Drittdienstleisters in einen TLPT gemäß Absatz 3 nachteilig auf die Qualität oder die Sicherheit von Dienstleistungen des IKT-Drittdienstleisters an Kunden, bei denen es sich um nicht in den Anwendungsbereich dieser Verordnung fallende Unternehmen handelt, oder auf die Vertraulichkeit in Bezug auf die mit diesen Dienstleistungen verbundenen Daten auswirkt, können das Finanzunternehmen und der IKT-Drittdienstleister unbeschadet Absatz 2 Unterabsätze 1 und 2 schriftlich vereinbaren, dass der IKT-Drittdienstleister unmittelbar vertragliche Vereinbarungen mit einem externen Tester schließt, um unter der Leitung eines benannten Finanzunternehmens einen gebündelten TLPT durchzuführen, an dem mehrere Finanzunternehmen beteiligt sind (gebündelter Test), für die der IKT-Drittdienstleister IKT-Dienstleistungen erbringt.

Diese gebündelten Tests erstrecken sich auf das relevante Spektrum von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von den Finanzunternehmen per Vertrag an die jeweiligen IKT-Drittdienstleister vergeben wurden. Die gebündelten Tests gelten als TLPT, die von den an den gebündelten Tests beteiligten Finanzunternehmen durchgeführt werden.

Die Zahl der Finanzunternehmen, die sich an den gebündelten Tests beteiligen, wird unter Berücksichtigung der Komplexität und der Art der betreffenden Dienstleistungen angemessen austariert.

(5) Finanzunternehmen wenden in Zusammenarbeit mit IKT-Drittdienstleistern und anderen beteiligten Parteien, einschließlich der Tester, jedoch ohne die zuständigen Behörden, wirksame Risikomanagementkontrollen an, um die Gefahr von potenziellen Auswirkungen auf Daten, Schäden an Vermögenswerten und Unterbrechungen kritischer oder wichtiger Funktionen, Dienste oder Vorgänge im Finanzunternehmen selbst, seinen Gegenparteien oder im Finanzsektor zu mindern.

(6) Nach Abschluss der Tests und der Ausarbeitung von Berichten und Plänen mit Abhilfemaßnahmen legen das Finanzunternehmen und gegebenenfalls die externen Tester der gemäß Absatz 9 oder 10 benannten Behörde eine Zusammenfassung der maßgeblichen Ergebnisse, die Pläne mit Abhilfemaßnahmen und die Unterlagen vor, mit denen belegt wird, dass der TLPT anforderungsgemäß durchgeführt wurden.

(7) Die Behörden stellen Finanzunternehmen eine Bescheinigung aus, aus der hervorgeht, dass der Test — wie in den Unterlagen nachgewiesen — im Einklang mit den Anforderungen durchgeführt wurde, um die gegenseitige Anerkennung bedrohungsorientierter Penetrationstests zwischen den zuständigen Behörden zu ermöglichen. Das Finanzunternehmen übermittelt der jeweils zuständigen Behörde die Bescheinigung, die Zusammenfassung der maßgeblichen Ergebnisse und die Abhilfemaßnahmen.

Unbeschadet einer solchen Bescheinigung bleiben Finanzunternehmen jederzeit in vollem Umfang für die Auswirkungen der in Absatz 4 genannten Tests verantwortlich.

(8) Finanzunternehmen beauftragen Tester für die Zwecke der Durchführung von TLPT gemäß Artikel 27. Ziehen Finanzunternehmen für die Zwecke der Durchführung von TLPT interne Tester heran, so beauftragen sie für jeden dritten Test einen externen Tester.

Kreditinstitute, die gemäß Artikel 6 Absatz 4 der Verordnung (EU) Nr. 1024/2013 als bedeutend eingestuft wurden, ziehen nur externe Tester gemäß Artikel 27 Absatz 1 Buchstaben a bis e heran.

Die zuständigen Behörden ermitteln Finanzunternehmen, die TLPT durchzuführen haben, unter Berücksichtigung der in Artikel 4 Absatz 2 aufgeführten Kriterien und stützen sich dabei auf die Bewertung von:

a) wirkungsbezogenen Faktoren, darunter insbesondere inwieweit sich die vom Finanzunternehmen erbrachten Dienstleistungen und ausgeführten Tätigkeiten auf den Finanzsektor auswirken;

b) etwaigen Bedenken hinsichtlich der Finanzstabilität, einschließlich des systemischen Charakters des Finanzunternehmens auf Unionsebene oder auf nationaler Ebene, je nach Sachlage;

c) dem spezifischen IKT-Risikoprofil, dem IKT-Reifegrad des Finanzunternehmens oder einschlägigen technologischen Merkmalen.

(9) Die Mitgliedstaaten können eine einzige staatliche Behörde für den Finanzsektor benennen, die auf nationaler Ebene für mit TLPT verbundenen Angelegenheiten im Finanzsektor zuständig ist, und betrauen sie mit allen diesbezüglichen Zuständigkeiten und Aufgaben.

(10) In Ermangelung einer Benennung gemäß Absatz 9 und unbeschadet der Befugnis zur Ermittlung der Finanzunternehmen, die verpflichtet sind, TLPT durchzuführen, kann eine zuständige Behörde die Wahrnehmung einiger oder aller in diesem Artikel oder in Artikel 27 genannten Aufgaben auf eine andere für den Finanzsektor zuständige nationale Behörde übertragen.

(11) Die ESA arbeiten im Einvernehmen mit der EZB im Einklang mit dem TIBER-EU-Rahmen gemeinsame Entwürfe technischer Regulierungsstandards aus, in denen Folgendes präzisiert wird:

a) die für die Zwecke der Anwendung von Absatz 8 Unterabsatz 2 herangezogenen Kriterien;

b) die Anforderungen und Standards für den Einsatz interner Tester;

c) die Anforderungen hinsichtlich:

   i) des Umfangs der in Absatz 2 genannten TLPT;

   ii) der Testmethodik und des Testkonzepts für jede einzelne Phase des Testverfahrens;

   iii) der Ergebnisse, des Abschlusses und der Behebungsphasen der Tests;

d) der Art der aufsichtlichen und sonstigen relevanten Zusammenarbeit, die für die Umsetzung von TLPT und die Erleichterung der gegenseitigen Anerkennung dieser Tests im Kontext von Finanzunternehmen, die in mehr als einem Mitgliedstaat tätig sind, erforderlich ist, um eine angemessene Beteiligung der Aufsichtsbehörden und eine flexible Umsetzung zu ermöglichen, damit den Besonderheiten finanzieller Teilsektoren oder lokaler Finanzmärkte Rechnung getragen wird.

Bei der Ausarbeitung dieser Entwürfe technischer Regulierungsstandards berücksichtigen die ESA gebührend etwaige Besonderheiten, die sich aus der unterschiedlichen Art der Tätigkeiten in verschiedenen Finanzdienstleistungssektoren ergeben.

Die ESA übermitteln der Kommission diese Entwürfe technischer Regulierungsstandards bis zum 17. Juli 2024.

Der Kommission wird die Befugnis übertragen, die vorliegende Verordnung durch Annahme der in Unterabsatz 1 genannten technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

Artikel 27

Anforderungen an Tester bezüglich der Durchführung von TLPT

(1) Finanzunternehmen ziehen für TLPT nur Tester heran, die

a) von höchster Eignung und Ansehen sind;

b) über technische und organisatorische Fähigkeiten verfügen und spezifisches Fachwissen in den Bereichen Bedrohungsanalyse, Penetrationstests und Red-Team-Tests nachweisen;

c) von einer Akkreditierungsstelle in einem Mitgliedstaat zertifiziert wurden oder formale Verhaltenskodizes oder ethische Rahmenregelungen einhalten;

d) eine unabhängige Gewähr oder einen Auditbericht in Bezug auf das zuverlässige Management von Risiken vorlegen, die mit der Durchführung von TLPT verbunden sind, darunter auch der angemessene Schutz vertraulicher Informationen des Finanzunternehmens und ein Ausgleich der geschäftlichen Risiken des Finanzunternehmens;

e) ordnungsgemäß und vollständig durch einschlägige Berufshaftpflichtversicherungen abgesichert sind, einschließlich einer Versicherung gegen das Risiko von Fehlverhalten und Fahrlässigkeit.

(2) Beim Einsatz interner Tester gewährleisten Finanzunternehmen, dass neben den Anforderungen in Absatz 1 auch folgende Bedingungen erfüllt sind:

a) der Einsatz wurde von der jeweils zuständigen Behörde oder von der gemäß Artikel 26 Absätze 9 und 10 benannten einzigen staatlichen Behörde genehmigt;

b) die jeweils zuständige Behörde hat überprüft, dass das Finanzunternehmen über ausreichende Ressourcen verfügt und sichergestellt hat, dass während der Konzeptions- und Durchführungsphase der Tests keine Interessenkonflikte entstehen; und

c) der Anbieter von Bedrohungsanalysen gehört nicht dem Finanzunternehmen an.

(3) Finanzunternehmen stellen sicher, dass in Verträgen, die mit externen Testern geschlossen werden, eine ordentliche Handhabung der Ergebnisse von TLPT vorgesehen ist und die diesbezügliche Datenverarbeitung, einschließlich Generierung, Speicherung, Aggregation, Entwurf, Berichterstattung, Weitergabe oder Vernichtung, keine Risiken für das Finanzunternehmen mit sich bringt.

KAPITEL V

Management des IKT-Drittparteienrisikos

Abschnitt I

Schlüsselprinzipien für ein solides Management des IKT-Drittparteienrisikos

Artikel 28

Allgemeine Prinzipien

(1) Finanzunternehmen managen das IKT-Drittparteienrisiko als integralen Bestandteil des IKT-Risikos innerhalb ihres IKT-Risikomanagementrahmens nach Artikel 6 Absatz 1 und im Einklang mit den folgenden Prinzipien:

a) Finanzunternehmen, die vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen für die Ausübung ihrer Geschäftstätigkeit getroffen haben, bleiben jederzeit in vollem Umfang für die Einhaltung und Erfüllung aller Verpflichtungen nach dieser Verordnung und nach dem anwendbaren Finanzdienstleistungsrecht verantwortlich.

b) Beim Management des IKT-Drittparteienrisikos tragen Finanzunternehmen dem Grundsatz der Verhältnismäßigkeit Rechnung, wobei Folgendes zu berücksichtigen ist:

i) die Art, das Ausmaß, die Komplexität und die Relevanz IKT-bezogener Abhängigkeiten,

ii) die Risiken infolge vertraglicher Vereinbarungen über die Nutzung von IKT-Dienstleistungen, die mit IKT-Drittdienstleistern geschlossen wurden, wobei die Kritikalität oder Relevanz der jeweiligen Dienstleistungen, Prozesse oder Funktionen sowie die potenziellen Auswirkungen auf die Kontinuität und Verfügbarkeit von Finanzdienstleistungen und -tätigkeiten auf Einzel- und Gruppenebene zu berücksichtigen sind.

(2) Finanzinstitute, bei denen es sich weder um die in Artikel 16 Absatz 1 Unterabsatz 1 genannten Unternehmen noch um Kleinstunternehmen handelt, beschließen im Rahmen ihres IKT-Risikomanagementrahmens eine Strategie für das IKT-Drittparteienrisiko und überprüfen diese regelmäßig, wobei gegebenenfalls die in Artikel 6 Absatz 9 genannte Strategie zur Nutzung mehrerer Anbieter Berücksichtigung findet. Die Strategie zum IKT-Drittparteienrisiko umfasst eine Leitlinie für die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden, und gilt auf individueller und gegebenenfalls teilkonsolidierter und konsolidierter Basis. Das Leitungsorgan überprüft auf der Grundlage einer Bewertung des Gesamtrisikoprofils des Finanzunternehmens und des Umfangs und der Komplexität der Unternehmensdienstleistungen regelmäßig Risiken, die im Zusammenhang mit den vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen ermittelt werden.

(3) Finanzunternehmen führen und aktualisieren im Rahmen ihres IKT-Risikomanagementrahmens auf Unternehmensebene sowie auf teilkonsolidierter und konsolidierter Ebene ein Informationsregister, das sich auf alle vertraglichen Vereinbarungen über die Nutzung von durch IKT-Drittdienstleister bereitgestellten IKT-Dienstleistungen bezieht.

Die vertraglichen Vereinbarungen gemäß Unterabsatz 1 werden angemessen dokumentiert, wobei zwischen Vereinbarungen, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen abdecken, und solchen unterschieden wird, bei denen dies nicht der Fall ist.

Finanzunternehmen erstatten den zuständigen Behörden mindestens einmal jährlich Bericht zur Anzahl neuer Vereinbarungen über die Nutzung von IKT-Dienstleistungen, den Kategorien von IKT-Drittdienstleistern, der Art der vertraglichen Vereinbarungen sowie den bereitgestellten IKT-Dienstleistungen und -Funktionen.

Finanzunternehmen stellen der zuständigen Behörde auf Verlangen das vollständige Informationsregister oder auf Anfrage bestimmte Teile dieses Registers zusammen mit allen Informationen zur Verfügung, die für eine wirksame Beaufsichtigung des Finanzunternehmens als notwendig erachtet werden.

Finanzunternehmen unterrichten die zuständige Behörde zeitnah über jede geplante vertragliche Vereinbarung über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen sowie in dem Fall, dass eine Funktion kritisch oder wichtig geworden ist.

(4) Vor Abschluss einer vertraglichen Vereinbarung über die Nutzung von IKT-Dienstleistungen müssen Finanzunternehmen:

a) beurteilen, ob sich die vertragliche Vereinbarung auf die Nutzung von IKT-Dienstleistungen zur Unterstützung einer kritischen oder wichtigen Funktion bezieht;

b) beurteilen, ob die aufsichtsrechtlichen Bedingungen für die Auftragsvergabe erfüllt sind;

c) alle relevanten Risiken im Zusammenhang mit der vertraglichen Vereinbarung ermitteln und bewerten, einschließlich der Möglichkeit, dass diese vertragliche Vereinbarung dazu beitragen kann, das in Artikel 29 genannte IKT-Konzentrationsrisiko zu erhöhen;

d) bei potenziellen IKT-Drittdienstleistern der gebotenen Sorgfaltspflicht nachkommen und während des gesamten Auswahl- und Bewertungsprozesses sicherstellen, dass der IKT-Drittdienstleister geeignet ist;

e) Interessenkonflikte, die durch die vertragliche Vereinbarung entstehen können, ermitteln und bewerten.

(5) Finanzunternehmen dürfen vertragliche Vereinbarungen nur mit IKT-Drittdienstleistern schließen, die angemessene Standards für Informationssicherheit einhalten. Betreffen diese vertraglichen Vereinbarungen kritische oder wichtige Funktionen, so berücksichtigen die Finanzunternehmen vor Abschluss der Vereinbarungen angemessen, ob die IKT-Drittdienstleister die aktuellsten und höchsten Qualitätsstandards für die Informationssicherheit anwenden.

(6) Bei der Ausübung der Zugangs-, Inspektions- und Auditrechte in Bezug auf den IKT-Drittdienstleister bestimmen Finanzunternehmen auf der Grundlage eines risikobasierten Ansatzes vorab die Häufigkeit von Audits und Inspektionen sowie die zu prüfenden Bereiche, indem allgemein anerkannte Auditstandards im Einklang mit etwaigen Aufsichtsanweisungen für die Anwendung und Einbeziehung solcher Auditstandards eingehalten werden.

Wenn vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen, die mit IKT-Drittdienstleistern geschlossen werden, ein hohes Maß an technischer Komplexität mit sich bringen, überprüft das Finanzunternehmen, dass die internen oder externen Revisoren oder ein Revisorenpool über die Fähigkeiten und Kenntnisse verfügen bzw. verfügt, die für die wirksame Durchführung der einschlägigen Audits und Bewertungen erforderlich sind.

(7) Finanzunternehmen stellen sicher, dass vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen gekündigt werden können, wenn einer der folgenden Umstände vorliegt:

a) ein erheblicher Verstoß des IKT-Drittdienstleisters gegen geltende Gesetze, sonstige Vorschriften oder Vertragsbedingungen;

b) Umstände, die im Laufe der Überwachung des IKT-Drittparteienrisikos festgestellt wurden und die als geeignet eingeschätzt werden, die Wahrnehmung der im Rahmen der vertraglichen Vereinbarung vorgesehenen Funktionen zu beeinträchtigen, einschließlich wesentlicher Änderungen, die sich auf die Vereinbarung oder die Verhältnisse des IKT-Drittdienstleisters auswirken;

c) nachweisliche Schwächen des IKT-Drittdienstleisters in Bezug auf sein allgemeines IKT-Risikomanagement und insbesondere bei der Art und Weise, in der er die Verfügbarkeit, Authentizität, Sicherheit und Vertraulichkeit von Daten gewährleistet, unabhängig davon, ob es sich um personenbezogene oder anderweitig sensible Daten oder nicht personenbezogene Daten handelt;

d) die zuständige Behörde kann das Finanzunternehmen infolge der Bedingungen der jeweiligen vertraglichen Vereinbarung oder der mit dieser Vereinbarung verbundenen Umstände nicht mehr wirksam beaufsichtigen.

(8) Für IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, richten Finanzunternehmen Ausstiegsstrategien ein. In den Ausstiegsstrategien wird den Risiken Rechnung getragen, die auf der Ebene der IKT-Drittdienstleister entstehen können, darunter insbesondere ein möglicher Fehler des IKT-Drittdienstleisters, eine Verschlechterung der Qualität der bereitgestellten IKT-Dienstleistungen, jede Unterbrechung der Geschäftstätigkeit aufgrund unangemessener oder unterlassener Bereitstellung von IKT-Dienstleistungen oder jedes erhebliche Risiko im Zusammenhang mit der angemessenen und kontinuierlichen Bereitstellung der jeweiligen IKT-Dienstleistungen oder der Beendigung vertraglicher Vereinbarungen mit IKT-Drittdienstleistern unter einem der in Absatz 7 genannten Umstände.

Finanzunternehmen stellen sicher, dass sie aus vertraglichen Vereinbarungen ausscheiden können, ohne:

a) Unterbrechung ihrer Geschäftstätigkeit,

b) Einschränkung der Einhaltung regulatorischer Anforderungen,

c) Beeinträchtigung der Kontinuität und Qualität ihrer für Kunden erbrachten Dienstleistungen.

Ausstiegspläne müssen umfassend, dokumentiert und im Einklang mit den in Artikel 4 Absatz 2 aufgeführten Kriterien ausreichend getestet sein sowie regelmäßig überprüft werden.

Finanzunternehmen ermitteln alternative Lösungen und entwickeln Übergangspläne, die es ihnen ermöglichen, dem IKT-Drittdienstleister die vertraglich vereinbarten IKT-Dienstleistungen und die relevanten Daten zu entziehen und sie sicher und vollständig alternativen Anbietern zu übertragen oder wieder in die eigenen Systeme zu überführen.

Finanzunternehmen verfügen über angemessene Notfallmaßnahmen, um die Fortführung der Geschäftstätigkeit zu gewährleisten, falls die in Unterabsatz 1 genannten Umstände auftreten.

(9) Die ESA erarbeiten über den Gemeinsamen Ausschuss Entwürfe technischer Durchführungsstandards, um die Standardvorlagen für die Zwecke des in Absatz 3 genannten Informationsregisters festzulegen, einschließlich Informationen, die allen vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen gemein sind. Die ESA übermitteln der Kommission diese Entwürfe technischer Regulierungsstandards bis zum 17. Januar 2024.

Der Kommission wird die Befugnis übertragen, die in Unterabsatz 1 genannten technischen Durchführungsstandards gemäß Artikel 15 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu erlassen.

(10) Die ESA erarbeiten über den Gemeinsamen Ausschuss Entwürfe für technische Regulierungsstandards, um den detaillierten Inhalt der Leitlinie, die in Absatz 2 in Bezug auf die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer und wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden, genannt wird, weiter zu spezifizieren.

Bei der Ausarbeitung dieser Entwürfe technischer Regulierungsstandards berücksichtigen die ESA die Größe und das Gesamtrisikoprofil des Finanzunternehmens sowie die Art, den Umfang und die Komplexität seiner Dienstleistungen, Tätigkeiten und Geschäfte. Die ESA übermitteln der Kommission diese Entwürfe technischer Regulierungsstandards bis zum 17. Januar 2024.

Der Kommission wird die Befugnis übertragen, die vorliegende Verordnung durch Annahme der in Unterabsatz 1 genannten technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

Artikel 29

Vorläufige Bewertung des IKT-Konzentrationsrisikos auf Unternehmensebene

(1) Bei der Ermittlung und Bewertung der in Artikel 28 Absatz 4 Buchstabe c genannten Risiken berücksichtigen Finanzunternehmen zudem, ob der geplante Abschluss einer vertraglichen Vereinbarung in Bezug auf IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, Folgendes herbeiführen würde:

a) Verträge mit einem IKT-Drittdienstleister, der nicht ohne Weiteres ersetzbar ist; oder

b) mehrfache vertragliche Vereinbarungen über die Bereitstellung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen mit demselben IKT-Drittdienstleister oder mit eng verbundenen IKT-Drittdienstleistern.

Finanzunternehmen wägen Nutzen und Kosten alternativer Lösungen ab, z. B. die Nutzung verschiedener IKT-Drittdienstleister, und berücksichtigen, ob und wie geplante Lösungen den geschäftlichen Erfordernissen und Zielen entsprechen, die in ihrer Strategie für digitale Resilienz festgelegt sind.

(2) Ist in der vertraglichen Vereinbarung über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen die Möglichkeit vorgesehen, dass ein IKT-Drittdienstleister IKT-Dienstleistungen zur Unterstützung einer kritischen oder wichtigen Funktion per Unterauftrag an andere IKT-Drittdienstleister vergibt, wägen Finanzunternehmen die Vorteile und Risiken ab, die im Zusammenhang mit einer solchen Unterauftragsvergabe entstehen können, insbesondere sofern der IKT-Unterauftragnehmer in einem Drittland niedergelassen ist.

Betreffen vertragliche Vereinbarungen IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, berücksichtigen die Finanzunternehmen gebührend die Bestimmungen des Insolvenzrechts, die im Falle der Insolvenz des IKT-Drittdienstleisters anwendbar wären, sowie jede Einschränkung, die sich im Zusammenhang mit der dringenden Wiederherstellung der Daten des Finanzunternehmens ergeben könnte.

Werden mit einem IKT-Drittdienstleister mit Sitz in einem Drittland vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen geschlossen, so beachten Finanzunternehmen neben den in Unterabsatz 2 genannten Umständen auch, dass die Datenschutzvorschriften der Union eingehalten und die Rechtsvorschriften in diesem Drittland wirksam durchgesetzt werden.

Ist in den vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen die Unterauftragsvergabe vorgesehen, so bewerten die Finanzunternehmen, ob und wie sich potenziell lange oder komplexe Ketten der Unterauftragsvergabe auf ihre Fähigkeit auswirken können, die vertraglich vereinbarten Funktionen vollständig zu überwachen, und ob die zuständige Behörde in dieser Hinsicht in der Lage ist, das Finanzunternehmen wirksam zu beaufsichtigen.

Artikel 30

Wesentliche Vertragsbestimmungen

(1) Die Rechte und Pflichten des Finanzunternehmens und des IKT-Drittdienstleisters werden eindeutig zugewiesen und schriftlich dargelegt. Der vollständige Vertrag umfasst die Vereinbarung über die Dienstleistungsgüte und wird in einem schriftlichen Dokument, das den Parteien in Papierform zur Verfügung steht, oder in einem Dokument in einem anderen herunterladbaren, dauerhaften und zugänglichen Format dokumentiert.

(2) Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen umfassen mindestens folgende Elemente:

a) eine klare und vollständige Beschreibung aller Funktionen und IKT-Dienstleistungen, die der IKT-Drittdienstleister bereitzustellen hat, wobei anzugeben ist, ob die Vergabe von Unteraufträgen für IKT-Dienstleistungen, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen, zulässig ist, und — wenn dies der Fall ist — welche Bedingungen für diese Unterauftragsvergabe gelten;

b) die Standorte — das heißt die Regionen oder Länder —, an denen die vertraglich vereinbarten oder an Unterauftragnehmer vergebenen Funktionen und IKT-Dienstleistungen bereitzustellen sind und an denen Daten verarbeitet werden sollen, einschließlich des Speicherorts, sowie die Auflage für den IKT-Drittdienstleister, das Finanzunternehmen vorab zu benachrichtigen, wenn er eine Änderung dieser Standorte beabsichtigt;

c) Bestimmungen über Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit in Bezug auf den Datenschutz, einschließlich des Schutzes personenbezogener Daten;

d) Bestimmungen über die Sicherstellung des Zugangs zu personenbezogenen und nicht personenbezogenen Daten, die von dem Finanzunternehmen im Fall einer Insolvenz, Abwicklung, Einstellung der Geschäftstätigkeit des IKT-Drittdienstleisters oder einer Beendigung der vertraglichen Vereinbarungen verarbeitet werden, sowie über die Wiederherstellung und Rückgabe dieser Daten in einem leicht zugänglichen Format;

e) Beschreibungen der Dienstleistungsgüte, einschließlich Aktualisierungen und Überarbeitungen;

f) die Verpflichtung des IKT-Drittdienstleisters, dem Finanzunternehmen bei einem IKT-Vorfall, der mit dem für das Finanzunternehmen bereitgestellten IKT-Dienst in Verbindung steht, ohne zusätzliche Kosten oder zu vorab festzusetzenden Kosten Unterstützung zu leisten;

g) die Verpflichtung des IKT-Drittdienstleisters, vollumfänglich mit den für das Finanzunternehmen zuständigen Behörden und Abwicklungsbehörden zusammenzuarbeiten, einschließlich der von diesen benannten Personen;

h) Kündigungsrechte und damit zusammenhängende Mindestkündigungsfristen für die Beendigung der vertraglichen Vereinbarungen entsprechend den Erwartungen der zuständigen Behörden und der Abwicklungsbehörden;

i) Bedingungen für die Teilnahme von IKT-Drittdienstleistern an den von den Finanzunternehmen angebotenen Programmen zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz gemäß Artikel 13 Absatz 6.

(3) Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen umfassen zusätzlich zu den in Absatz 2 genannten Elementen mindestens Folgendes:

a) vollständige Beschreibungen der Dienstleistungsgüte, einschließlich Aktualisierungen und Überarbeitungen, mit präzisen quantitativen und qualitativen Leistungszielen innerhalb der vereinbarten Dienstleistungsgüte, um dem Finanzunternehmen eine wirksame Überwachung von IKT-Dienstleistungen und das unverzügliche Ergreifen angemessener Korrekturmaßnahmen zu ermöglichen, wenn eine vereinbarte Dienstleistungsgüte nicht erreicht wird;

b) Kündigungsfristen und Berichtspflichten des IKT-Drittdienstleisters gegenüber dem Finanzunternehmen, einschließlich der Meldung aller Entwicklungen, die sich wesentlich auf die Fähigkeit des IKT-Drittdienstleisters, IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen gemäß den vereinbarten Leistungsniveaus wirksam bereitzustellen, auswirken könnten;

c) Anforderungen an den IKT-Drittdienstleister, Notfallpläne zu implementieren und zu testen und über Maßnahmen, Tools und Leit- und Richtlinien für IKT-Sicherheit zu verfügen, die ein angemessenes Maß an Sicherheit für die Erbringung von Dienstleistungen durch das Finanzunternehmen im Einklang mit seinem Rechtsrahmen bieten;

d) die Verpflichtung des IKT-Drittdienstleisters, sich an den in den Artikeln 26 und 27 genannten TLPT des Finanzunternehmens zu beteiligen und uneingeschränkt daran mitzuwirken;

e) das Recht, die Leistung des IKT-Drittdienstleisters fortlaufend zu überwachen, wozu Folgendes gehört: